



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/590,438	06/09/2000	Terence V. Trench	VISAP060	1408
22434	7590	02/02/2004	EXAMINER	
BEYER WEAVER & THOMAS LLP P.O. BOX 778 BERKELEY, CA 94704-0778			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	3

DATE MAILED: 02/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	09/590,438		TRENCH, TERENCE V.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Jung W Kim		2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) 13-18 and 20 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 and 19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☒ Claim(s) 1-20 are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 June 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All   b) ☐ Some \*   c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                  | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). ____.  |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                         | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>2</u> . | 6) <input type="checkbox"/> Other: _____                                    |

### DETAILED ACTION

1. Claims 1-12 and 19 have been examined.

#### ***Election/Restrictions***

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:
  - I. Claims 1-12 and 19, drawn to a method of creating a digital certificate, classified in class 713, subclass 175.
  - II. Claims 13-18 and 20, drawn to a method of authenticating a user by presenting a chip card to an entity, classified in class 713, subclass 159.

The inventions are distinct, each from the other because of the following reasons:

3. Inventions in Group I and Group II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed (Group II) does not require the particulars of the subcombination as claimed (Group I) because the method of authenticating a user disclosed in claims 13-18 and 20 do not require the specific method of creating a digital certificate disclosed in claims 1-12 and 19. The subcombination has separate utility such as a method of creating a digital certificate.

4. In a telephone reply from Justin White on January 20, 2004 a provisional election was made to prosecute the invention of Group I, claims 1-12 and 19; however, no indication was given if the election was made with or without traverse. The Office will assume that the election was made without traverse. Affirmation of this election must be made by applicant in replying to this Office action. Claims 13-18 and 20 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

### ***Drawings***

5. New corrected drawings are required in this application because Figures 1-3 are informal. Applicant is advised to employ the services of a competent patent draftsman outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings.

6. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the steps of accessing the digital certificate in the certificate library using the issuing-party identifier (claim 5) or a merchant-specific identifier (claim 6) must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

7. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "202" has been used to designate both a certificate library and a certificate library directory (see Figures 2 and 3).

8. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

### ***Specification***

9. The disclosure is objected to because of the following informalities: on page 9, lines 15-17, the sentence is not grammatical; on page 5, line 10, the acronym "DED" should be "DES". Reference No. 202 is identified as a certificate library and a certificate library directory (see page 13, line 16 and page 14, line 25), however, Reference No. 202 can only designate one portion of the invention. On page 16, line 1, the specification identifies a certificate library directory with Reference Number 322; there is no Reference No. 322 in the Figures. Appropriate correction is required.

10. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The following title is suggested: "Method of creating and storing one or more digital certificates assigned to a subscriber for efficient access using a chip card".

***Claim Rejections - 35 USC § 112***

11. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

12. Claims 4 and 6 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Regarding claim 4, the disclosure specifies using a DES shared-key system to configure a digital certificate and an associated certificate chain in an alternative embodiment to one utilizing a PKI configuration. However, PKI is a collection of protocols to provide key distribution infrastructure, whereas DES shared-key system is a means to provide cryptographic protection using symmetric keys and not an obvious means to configure a digital certificate and an associated certificate chain. Furthermore, the specification does not elaborate how the DES shared-key system can be used to configure the digital certificate and the associated certificate chain. Regarding claim 6, the disclosure does not specify a step of accessing a digital certificate in the certificate library using a merchant-specific identifier.

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 1 and 2 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

15. The step of "associating a user public key with the first data" in claim 1 and the step of "associating a certificate chain with the digital certificate" in claim 2 are relative steps which renders the claim indefinite. The association steps are not defined by the claims, the specification does not provide a standard for ascertaining the association, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

16. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: creating a plurality of PKIs associated with the user for storage in the user-allotted memory segment of the certificate library.

17. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: claim 6 specifies using a "merchant-specific identifier" to access the certificate (claim 6, line 5); however, the

claim does not specify the relationship of a merchant-specific identifier with the data pertaining to a user or useful to an issuing party (claim 1, lines 4-5).

***Claim Rejections - 35 USC § 103***

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

19. Claims 1, 2, 5, 9, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2<sup>nd</sup> Edition (hereinafter Stallings) in view of VeriSign Certification Practice Statement Version 1.2 (hereinafter VeriSign). As per claim 1, Stallings teaches a method of creating a digital certificate for a user comprising:

- a. creating a digital certificate containing a user public key, a first data set, and an encrypted second data set, the digital certificate being identifiable by an issuing-party identifier (see Stallings, page 342 and 345, Figures 11.3 and 11.4 and related text);
  - i. whereupon the user public key and corresponding private key is generated prior to the creation of the digital certificate by the issuing party (see Stallings, page 341, 6<sup>th</sup> paragraph, last sentence),
  - ii. and the first data set contains data pertaining to the user and useful to an issuing party issuing the digital certificate (see Stallings, page 342,



- bullets: Issuer name, Subject name, Subject's public-key information, Issuer unique identifier, Subject unique identifier),
- iii. and the encrypted second data set is a hash of the user public key combined with the first data and encrypted by an issuer private key (see Stallings, page 342, bullet: Signature);
- b. storing the digital certificate at a user-allotted memory segment of a certificate library, in which one or more digital certificates for the user can be stored at the user-allotted memory segment (see Stallings, page 341, 1<sup>st</sup> and 2<sup>nd</sup> paragraphs).

Stallings is silent on the matter of deriving the first data set. However, virtually all Certificate Authorities requires in some fashion a means to obtain subscriber's information. VeriSign, for example, derives the information from a securely transmitted application filed by the user (see VeriSign, Section 4.2). It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a step to derive data pertaining to a user by the issuer of the digital signature. Motivation for such an implementation would enable users to subscribe to the CA certificate creation and distribution services. The aforementioned covers claim 1.

20. As per claim 2, Stallings covers a method of creating a digital certificate for a user as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the digital certificate is a part of a certificate chain, wherein the certificate chain has a trusted root, the trusted root being different from other trusted roots stored at the user-

allotted memory segment (see Stallings, page 345, Figure 11.4; see VeriSign, Section 2.5).

21. As per claim 5, Stallings covers a method of creating a digital certificate for a user as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, an issuing party identifier is used to access the digital certificate (see Stallings, pages 343-345, 'Obtaining a User's Certificate', especially Steps 1, 2, and Figure 11.4).

22. As per claim 9, Stallings covers a method of creating a digital certificate for a user as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, based on the applicant's definition of an authentication challenge value (see page 11, lines 13-14), the method further includes presenting a string to be signed by the corresponding user's private key (see Stallings, page 346, Figure 11.5 (c), nonce 'rB').

23. As per claim 10, Stallings covers a method of creating a digital certificate for a user as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the cryptographic infrastructures listed in claim 10 are necessary implementations for a digital signature to be created then stored as claimed in claim 1.

24. Claims 7, 8, 11, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of VeriSign, and further in view of Hughes "Certificate Inter-operability – White Paper" (hereinafter Hughes). As per claims 7 and

8, Stallings covers a method of creating a digital certificate for a user as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose verifying the signature of a certificate. However, the steps disclosed in claim 7 and 8 are typical procedures to validate a signature of a certificate. For example, Hughes teaches a simple validation routine on a digital signature which includes finding the issuer's name from the certificate and locating the issuer's public key from another digital certificate, then using the public key to validate that the certificate signature was generated by the issuer (see Hughes, page 224, 1<sup>st</sup> paragraph, steps 1-3). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Hughes to the invention covered by Stallings. Motivation for such an implementation would utilize a standard and simple means of signature verification. The aforementioned covers claims 7 and 8.

25. As per claim 11, Stallings covers a method of creating a digital certificate for a user as outlined above in the claims 8 and 10 rejections under 35 U.S.C. 103(a). In addition, Hughes teaches that distribution of certificates by means of a smartcard is a standard means of manually distributing certificates (see Hughes, page 225, final paragraph, 'Manual Distribution').

26. As per claim 12, Stallings covers a method of creating a digital certificate for a user as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition,

Hughes teaches that certificate libraries are typically in the form of an LDAP server (see Hughes, page 230, step 1).

27. Claims 3 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of VeriSign, and further in view of Sudia U.S. Patent No. 5,659,616 (hereinafter Sudia). As per claim 3, Stallings covers a method of creating a digital certificate for a user as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). In addition, the method further includes using the Public Key Infrastructure (PKI) to configure the digital certificate and the associated certificate chain, thereby creating one PKI (see VeriSign, Section 1.1 and Section 2.5). Both Stallings and VeriSign are silent on the matter of storing two or more PKIs at the user-allotted memory segment of the certificate library. However, at the time the invention was made, attribute certificates were disclosed as another option to identity-based certificates. As disclosed by Sudia, attribute certificates are linked to a user's public key certificate but are separate entities from the public key certificate since the separation of duties may require that a different CA issue the attribute certificate (see Sudia, col. 4, lines 10-39). In this scenario, a plurality of certificates sharing the same public key would be issued for a user and published in the certificate library. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Sudia to the invention taught by Stallings. Motivation for such an implementation would enable the storage of a plurality of attribute certificates corresponding to a user's public key

certificate and thus enable a binding of the public key of the user to different roles or duties as taught by Sudia.

28. As per claim 19, Stallings covers a certificate library having a plurality of user-specific memory segments, each user-specific memory segment storing a plurality of digital certificates issued to a user, each digital certificate identifiable by an issuer-identifier and being associated with a trusted root certificate and each digital certificate having the same user public key as outlined in the claim 3 rejection under 35 U.S.C. 103(a).

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ramasubramani et al. U.S. Patent No. 6,233,577.

Ellison "Generalized Certificates".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

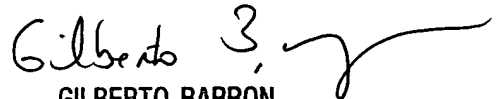
Art Unit: 2132

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



Jung W Kim  
Examiner  
Art Unit 2132

Jk  
January 23, 2004



GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100